Illustration réalisée par « Le Soir » sur base d'échanges réels tenus sur Sky ECC en janvier 2020. Les protagonistes étaient basés dans la région de Besançon (Besac).

net) et leur communication aux autorités. Ce texte, dont deux versions ont été cassées par la Cour constitutionnelle pour non-respect de la vie privée, prévoit un cadre autour de la conservation des données téléphoniques par les opérateurs de manière à permettre à la justice de demander de telles données si nécessaire. Il ne s'agit pas du contenu des conversations, mais bien des métadonnées : qui communique ? Avec qui ? Quand et où ? Une (petite) étape face à ce qui se trame au niveau européen…

Europol, future NSA européenne

Un pas crucial a ainsi été franchi en février 2022, à la faveur du dossier Sky ECC : la réforme d'Europol, promise à se muer en véritable NSA européenne. Quelques mois plus tôt, l'agence avait été sommée par l'European Data Protection Board (la tutelle des autorités de protection des données) d'effacer toutes nouvelles données reçues par les Etats membres, sans rapport avec des activités criminelles. Et celles qu'elle conservait déjà depuis plusieurs années illégalement (sans rapport avec des activités criminelles, donc). Parmi ces masses babyloniennes de data : les fiches de demandeurs d'asile n'ayant jamais été impliqués dans aucun crime. Mais aussi ces fameuses données issues des services de messageries cryptées, aspirées parfois à l'aveuglette. Dont celles de Sky ECC. Le Conseil européen et le Parlement sont finalement passés outre ces injonctions pour élargir le mandat d'Europol et l'autoriser à conserver ces masses de données.

« Ils avaient besoin de légaliser certaines pratiques de l'Agence européenne qui, jusque-là, étaient jugées illégales, comme le fait de traiter des données de personnes qui n'ont rien à voir avec des activités criminelles », justifie Chloé Berthélémy (Edri). De quoi, en quelque sorte, transformer Europol en « machine à blanchir les données ». « Pourquoi ? Parce que les Etats membres utilisaient de plus en plus Europol pour stocker le résultat d'opérations de hacking de masse. Ces quantités de données non filtrées, collectées en masse sur tous les utilisateurs, criminels et non criminels, étaient donc transférées à Europol. » Au cas où… Il s'agit là, précisément, d'un des ingrédients majeurs du programme de surveillance de masse de la NSA révélé en 2013 par Edward Snowden. Ces données doivent aussi servir à entraîner les modèles d'intelligence artificielle utilisés par Europol pour ses programmes de surveillance.

Ceci n'offre toujours pas de « front door » pour mettre « sur écoute », en toute légitimité, WhatsApp ou Signal. L'offensive viendra de l'ex-commissaire européenne aux Affaires intérieures, Ylva Johansson. La Suédoise a fait de la lutte contre les contenus à caractère pédopornographique le combat d'un mandat. Une croisade qui l'a amenée à présenter un projet de directive qui obligerait les fournisseurs de services en ligne à surveiller automatiquement, et sans discrimination, l'ensemble des communications numériques. Y compris celles des messageries dites « cryptées de bout en bout », comme WhatsApp ou Signal. En clair, obliger les plateformes à scanner tous les contenus des messages privés afin de détecter d'éventuelles images illicites. Le logiciel mouchard partagerait le contenu et signalerait automatiquement les utilisateurs suspects aux autorités judiciaires. Le nom donné à ce projet de règlement, très vite dénoncé par la Cour de Justice européenne : « Chat Control ».

« Un modèle pour les Etats autoritaires »

Des centaines de chercheurs en cryptographie se sont dressés vent debout contre ce texte, le jugeant techniquement illusoire et, surtout, inefficace, tant les possibilités pour les criminels de contourner la censure étaient à portée de main. 48 élus européens ont signé une lettre ouverte, rédigée par l'ex-député allemand (Parti pirate) Patrick Breyer, principal opposant du texte, dénonçant « un projet de surveillance de masse » qui constituerait « un modèle pour les Etats autoritaires ». Plusieurs présidences du Conseil de l'UE, dont la Belgique, en faveur du texte, se sont finalement cassé les dents pour le faire adopter. Mais il est toujours sur le feu.

L'idée d'élargir la directive Chat Control à l'ensemble des contenus (pas seulement à la détection de contenus pédocriminels) échangés sur les messageries privées est aussi clairement dans l'air. Mi-2022, Europol a ainsi demandé à la Commission un accès illimité aux données issues de la détection et du scanning des communications. Et qu'aucune limite ne soit imposée sur l'utilisation de ces données. La fin du cryptage, donc.

Le programme « Going Dark »

La lame de fond est clairement là. En témoigne encore la réflexion sur un programme de surveillance initié en 2023 par la présidence, et partagé de manière assez homogène par l'ensemble des Etats membres ainsi qu'Europol, surfant sur le succès judiciaire de l'opération Sky ECC. Son nom est explicite, « Going Dark ». Soit, l'obligation pour les services de messageries de ménager cette fameuse « porte dérobée » permettant aux agences de renseignements de suivre, légitimement, les communications occultes de personnes jugées suspectes d'activités criminelles.

Le problème, dénoncent en chœur les opposants au projet, c'est qu'une messagerie cryptée qui, par défaut, offre une faille de sécurité pour malgré tout y pénétrer, n'est plus une messagerie cryptée. De facto, ceux qui utiliseraient un vrai service crypté, se mettraient hors-la-loi. « Une porte dérobée sécurisée, ça n'existe pas. Mathématiquement, vous ne pouvez pas à la fois diminuer le chiffrement, c'est-à-dire le contourner, et à la fois garantir le même niveau de sécurité que le chiffrement offre », avance Chloé Berthélémy.

Alors que l'ONU a reconnu le chiffrement comme un droit humain, le programme « Going Dark » entend sonner le glas de WhatsApp et Signal, l'une des messageries les plus sécurisées, plébiscitée par les journalistes et les défenseurs des droits humains. La présidente de la fondation Signal, Meredith Whittaker, a prévenu : si Chat Control ou toute autre disposition visant à affaiblir le chiffrement de bout en bout était adoptée, elle quitterait le marché européen.

fait l'objet d'aucune perquisition. Le Canada, réputé pour sa législation pointilleuse en matière de vie privée, va rejeter les requêtes du juge français, pointant des « informations insuffisantes ». « L'équipe commune d'enquête ne voulait pas donner l'opportunité à Sky de coopérer », appuient les avocats français de Jean-François Eap, Stéphane Bonifassi et Marie Poirot. « Si l'entreprise avait transmis les quelques métadonnées qu'elle avait dans le cadre d'une demande officielle, le storytelling de l'entreprise criminelle n'aurait plus tenu debout. »

42 discussions suspectes

La méthode utilisée par les autorités pour déterminer que les 170.000 utilisateurs de Sky ECC étaient tous criminels sème aussi le doute. Dans un P.V. de la police judiciaire fédérale, établi à la demande du juge d'instruction malinois Philippe Van Linthout, et que *Le Soir* a en sa possession, la méthode d'échantillonnage s'est opérée en deux temps. Un premier échantillon de 21 discussions interceptées au niveau mondial, a raison de plus ou moins une par mois. Et un second échantillon aléatoire de 21 conversations centrées sur les distributeurs de Sky ECC et les utilisateurs belges (ou ayant été « bornés » en Belgique). Soit un total de 42 échanges étudiés… sur un milliard de messages interceptés.

Comme ces 42 conversations contenaient toutes des photos de nature criminelle (principalement des images de cannabis ou de cocaïne, mais aussi quelques armes à feu et des scènes d'ultra violence), la présomption de culpabilité a été extrapolée au milliard de messages. Si la petite taille de l'échantillon étudié interroge, en termes de représentativité, cela n'empêche pas les auteurs du PV d'écrire : « En conclusion (…), les rédacteurs estiment pouvoir dire qu'il n'y a pas, en tout cas de manière aléatoire, un code PIN qui ne puisse pas être lié d'une quelconque manière, au moins par des photos, à des faits qui semblent manifestement criminels. »

Le timing du PV est aussi interpellant : rédigé le jeudi 18 mars 2021, il intervient clairement en aval de l'interception (qui a débuté le 24 juin 2019). Mais surtout, plus d'un mois après la phase d'écoute en direct où les enquêteurs pouvaient déchiffrer en temps réel les conversations de tous les utilisateurs, suspects ou légitimes.

La police n'avait aucune idée de l'identité des 170.000 utilisateurs et utilisatrices dont ils ont collecté les données pendant plus d'un an. Ils ont juste lancé un filet de pêche et récupéré toutes les données

Chloé Berthélémy
Conseillère politique à l'European Digital Rights

Un certificat d'innocence

Les enquêteurs auraient-ils pris conscience trop tard qu'ils étaient en dehors des clous pour justifier une interception indiscriminée, ne respectant pas les bases juridiques du principe de proportionnalité ? Un fait, pour le moins troublant, sinon surréaliste, appuie cette thèse. Le 10 mars 2021, dans la foulée de la conférence des autorités judiciaires annonçant le démantèlement du réseau Sky ECC, le parquet fédéral et celui de Malines se sont fendus d'un communiqué de presse dans lequel ils informent les utilisateurs de Sky ECC que leurs données ont été écoutées. Il invite surtout les entreprises et les particuliers « qui utiliseraient les services Sky ECC à des fins légitimes » de se présenter à la police. Et ce, pour s'assurer que leurs données ne fassent plus l'objet d'une enquête policière plus poussée. A charge donc, pour les utilisateurs, d'aller eux-mêmes chercher une sorte de certificat d'innocence. Ce qui, en somme, revient à transformer la présomption d'innocence (tout le monde est innocent jusqu'à preuve du contraire) en présomption de culpabilité.

« La police n'avait aucune idée de l'identité des 170.000 utilisateurs et utilisatrices dont ils ont collecté les données pendant plus d'un an. Ils ont juste lancé un filet de pêche et récupéré toutes les données », soutient Chloé Berthélémy, conseillère politique à l'European Digital Rights (Edri), fédérant la plupart des organisations de défense des droits humains. « Avec Sky ECC, chaque utilisateur a été désigné comme suspect par défaut parce qu'il possède un téléphone Sky ECC. C'est ce qu'on appelle une interception de masse, soit la collecte massive indiscriminée. Le fait qu'on puisse dire qu'on vit dans une société démocratique veut dire qu'aussi on respecte nos droits fondamentaux, donc le droit à un procès équitable et le droit à la présomption d'innocence. Sinon, on vivrait dans un régime autoritaire. »